Cybersecurity Crisis-Planning Checklist

Tips for Planning and Ensuring Business Continuity with Zscaler

zscaler™

In uncertain times, a CxO's first priority is to protect the health and well-being of employees and communities. Enterprises must be agile, not only in development, but in operations, and never more so than when a disaster hits. Crises may disrupt operations, but adjusting to a crisis-induced "new normal" cannot result in a compromise to cybersecurity.

In an emergency situation, a CISO must act fast and decisively. Zscaler identifies eight key strategic objectives for CISOs in times of crisis:

1. Enable and support employee remote work. →
2. Enable and support security operations and monitoring teams' remote work. →
3. Plan for increased cyberthreat risks, particularly situational attacks. →
4. Verify third-party vendors can support your systems. →
5. Adjust business-security priorities. →
6. Plan for budget adjustment and scrutiny. →
7. Ensure regulatory compliance, even if adherence is made more difficult. →
8. Lead in a time of change. →

Every crisis event is different. The following checklist is a blueprint for CISO crisis management.

1. Enable and support employee remote work.

In a crisis—particularly a viral outbreak—employees must be able to work remotely. CISOs must address the following considerations.

☐ How will employee remote work affect data center operations?

- Patch and update workflows may be disrupted without hands-on effort:
  - Review and establish processes to patch and manage systems remotely.
- Investigating cyber breaches and compromised devices must be done remotely:
  - Create new processes for cyber-remediation personnel working remotely.
  - Create new investigation and forensics processes for remote employees and assets.
  - Triage: Prioritize investigations and focus on crucial initiatives first.
- With no one on-premises, office wireless networks become an attractive breach point for hackers:
  - Ensure on-premises wireless networks can be secured remotely, or shut down remotely if not needed.

☐ Will service and product licensing support shift to remote work?

- Determine if endpoint license counts will change with an increase in remote work.
- Determine if cybersecurity tool (including anti-virus, endpoint detection and response, identity access and management) license counts will change with an increase in remote work.
- Determine if remote-work shift to BYOD access will affect license counts.

☐ How will an enterprise shift to remote work affect device security controls?

- Determine how remote work will affect your security controls:
  - Do a control inventory (use NIST Cybersecurity Framework as a guide) and analysis.
- Verify controls work remotely:
  - Data-center-based controls may no longer be effective without using VPN (which could be over-loaded with spikes in remote access).
  - If necessary, identify compensating controls (administrative/technical).
  - Determine risk, impact to data loss prevention (DLP) mechanisms.

- Establish a response plan for lost visibility:
  - Determine alternative ways to receive telemetry, as you may no longer be able to communicate with endpoints.
  - Ensure default update mechanisms are enabled.

☐ How will you handle malware cleanup?

- Establish a way to clean remote endpoints. If this isn't possible, establish a workflow for employees to process devices.

☐ How will you reinforce a security culture without in-person communication, events?

- Establish a process to evangelize education, cybersecurity best practices.
- Add a "security brief" to scheduled senior executive communications.

2. Enable and support security operations and monitoring teams' remote work.

Your data center and security teams are also working from home while helping employees adjust. This can impact security and IT workflows.

☐ How will you communicate and disseminate information to remote IT teams?

- Establish email lists, group chats, regular (virtual) meetings.
- Employ conferencing tools like Zoom or WebEx.
- Invest in collaboration tools like Slack, Microsoft Teams, or Google Chat.

☐ How will IT teams access tools and monitoring from home?

- Modify access policy rules to allow remote use.
- Use web front-ends or client applications for remote access if possible.

☐ How will incident response change?

- Establish a plan to respond to remote security incidents.
- Set up a remediation plan for fixing remote incidents.

☐ How will you provision/deprovision identity?

- Ensure employee access can be granted/revoked remotely.
- If necessary, reduce privileges as a risk-mitigation strategy.
- Define a plan if a "starters, leavers, and movers" (SLAM) process requires a physical presence for the employee or onboarding staff, including:
  - Asset distribution or reclamation
  - Asset cleaning (physically and logically)
  - Document-signing
- If necessary, be prepared to distribute Token/MFA mechanisms via post or parcel systems.

☐ How will working from home affect third-party security services?

- Determine and document third-party access requirements.
- Prioritize third-party access by urgency, immediacy.
- Establish a workflow for granting and revoking third-party access.

3. Plan for increased cyberthreat risks, particularly situational attacks.

Crises like the 2020 COVID-19 outbreak typically lead to an increase in so-called "situational" malware attacks.

When enterprises that employ VPNs for remote access increase remote work, they extend both MPLS-backhauling distance and threat surface. VPN-based perimeter security models can't easily scale to support increased remote access, and some employees may be tempted to bypass firewalls to egress to the internet. Hackers recognize such vulnerabilities, and take advantage. Worse, crisis information can saturate media, and reduce security awareness: cynical scammers try to deploy malware masked as important crisis communications.

Cybersecurity experts (like Zscaler's own ThreatLabZ team) correlate crises with data-breach increases. CISOs must address new threat risks that arise in times of crisis.

☐ Gauge risk: are remote users vulnerable to phishing or other ploys?

- Reiterate security policies to employees, and apprise them of crisis-related scams.
- Evangelize the importance of security diligence in an emergency.

4. Verify third-party vendors can support your systems.

Third-party security vendors will adjust operations to meet crisis demands as well. Communicate with your third-party vendors and verify that their support of your systems isn't changing in any way that affects your environment.

☐ Will security vendors support your crisis-adjusted operations?

- Audit third-party vendor support:
  - Ensure third-party system access is preserved, even if remote.
  - Review each vendor's Business Continuity Planning (BCP) readiness and crisis-service plans.
  - Note that Managed Security Service Providers (MSSP) in particular might lack work-from-home capabilities. How can you plan for that risk?

5. Adjust business-security priorities.

In a crisis, an enterprise must focus on emergency response, and cybersecurity priorities can receive less attention.

☐ How do you maintain security during change?

- If necessary, adjust the acceptable risk levels for company assets:
  - Inventory physical assets and logical assets.
  - Ensure as much visibility as possible into asset risk contributors.
  - Assess performance vs. security, and adjust security posture as needed.
- Evaluate your risk tolerance given a shift to remote work.
- Remain an advocate for security without blocking needed changes or actions. (Security will remain crucial to long-term success.)

☐ Can you see new processes, deployments, and devices?

- Establish mechanisms to obtain, consume, and evaluate reports (feeds, logs, telemetry) remotely.
- Establish processes to act on that information from systems outside the enterprise.

6. Plan for budget adjustment and scrutiny.

In a crisis, spending on emergency response can take precedence over security. Project funding may disappear, or at least be harder to obtain. Security may even be deprioritized to address immediate operational needs.

☐ Will there be an impact to your operational or planning budget?

- Inventory, prioritize, and if necessary, triage essential plans, devices, and services.
- Be prepared to cut non-essentials (and accept new definitions of what constitutes "essential").
- Repurpose travel, event, and future initiatives budget to supplement security priorities.

7. Ensure regulatory compliance, even if adherence is made more difficult.

Even in a crisis, enterprise regulatory compliance remains a mandate.

☐ How will operational and structural changes in response to a crisis affect your organization's ability to comply with regulatory requirements?

- Determine, then document how new device and process deployments will impact data flows and security requirements.

☐ Will your organization's ability to comply with data-residency requirements be impacted by crisis-response operations?

- Determine where data-at-rest lives and how data-in-transit paths may change.
- Verify that compliance is maintained across new data flow paths. This may require changes to cloud and data-center administration, and even adding new data redundancy in different geos.
- Ensure SSL and other security measures are employed as necessary, and comply with applicable data-privacy statutes.

☐ Will regulatory bodies or governments adjust compliance rules in times of crisis?

- Monitor regulatory communications that affect compliance requirements.
- Build (or at least plan to build) response workflows in the case of crisis-based compliance requirement adjustments.

8. Lead in a time of change.

In a crisis, everyone works without enough information, and must react to events as they happen. Given the imperative of preserving security, a CISO can never act out of panic. Effective crisis communications require perspective, humility, directness, and a strong voice: over-communicating without specific purpose becomes noise, but under-communicating creates information vacuums. Establish and communicate clear plans of action.

☐ With whom will you need to communicate?

- Ensure internal security stakeholders are clear on roles, responsibilities, actions, and processes.
- Ensure external stakeholders and customers are notified of changes that affect operations.

☐ How frequently will you need to communicate?

- Communicate important and immediate changes when they happen.
- Communicate plans in measurable, trackable phases, with clear metrics and progress gates.
- Ensure communication is not just broadcast, but received, understood, and acted upon. Establish workflows to measure communication efficacy.

☐ With whom will you coordinate communication?

- Establish an internal crisis communication team.
- Consult industry groups to benchmark communications best practices.
- Research relevant governmental resources (local, state, or federal).

☐ How can a CISO best provide leadership in crisis communications?

- As a security professional, you're experienced in crisis management:
  - Guide your organization's preparations and response.
  - Help your organization stakeholders assess the consequences of emergency decisions.
- Provide calm leadership:
  - Combat anxiety, uncertainty, and panic with knowledge, understanding, and preparation.

Zscaler's cloud-built, secure access service edge platform was designed specifically to enable direct connectivity via local internet breakouts, ensuring that enterprises (and all those enterprises' remote workers) can move forward in uncertain times.

Zscaler's Business Continuity Program helps organizations maintain a best-in-world security stance under even the most-challenging circumstances.

Learn more

About Zscaler

Zscaler was founded in 2008 on a simple but powerful concept: as applications move to the cloud, security needs to move there as well. Today, we are helping thousands of global organizations transform into cloud-enabled operations.